*Jurnal Dinamika Universitas Muhammadiyah Tangerang*
*Tangerang, April 2022, pp 21-29*

*P ISSN : 2477-1546*
*E ISSN : 2581-1894*

# Analisa Penggunaan Teknik Advanced Encryption (AES) dalam Kriptografi

**Adnan Rasidin[1], Ahmad Jati Nugroho[2]**
Program Studi Teknik Informatika, Universitas Muhammadiyah Tangerang, Cikokol
Program Studi Teknik Informatika, Universitas Muhammadiyah Tangerang, Cikokol

Co Responden Email : adnan.rasidin74@gmail.com

Received 01-01-2022
Revised 01-03-2022
Accepted 25-03-2022
Available online 01 -04-2022

***Kata Kunci:*** *AES, algoritma AES, algoritma kunci simetris, enkripsi file..*

***Abstrak:*** *AES atau kepanjangan dari Cryptography Advanced Encryption Standard digunakan untuk mengenkripsi file dan dokumen. AES adalah algoritma kriptografi merupakan algoritma yang mengenkripsikan kunci simetris standar yang digunakan pada saat ini. AES-128 memiliki 1 blok plaintext 128-bit dan proses algoritma kriptografi terlebih dahulu mengubah plaintext menjadi array heksadesimal 4 x 4 yang bisa disebut sebagai state, dimana setiap state elemen berukuran 1 bit. Pada proses mengenkripsi ke dalam AES melibatkan transisi status berulang kali dalam 10 langkah. Setiap putaran AES hanya membutuhkan 1 hasil kunci dari pembangkitan kunci menggunakan 2 kunci transformasi, transformasi dan penggantian. Enkripsi AES menggunakan 4 perubahan dalam urutan berikut: sub-byte, shift, kolom campuran, dan kunci tambahan. Sebaliknya, proses dekripsi menggunakan kebalikan dari transformasi dasar dari algoritma AES, kecuali untuk pengunci ekstra. Jadi urutan transformasi pada deskripsi adalah shiftrows, sub-bytes, mix column, dan addroundkey. Pada data teks, proses pengkodean dimulai dengan mengubah data teks menjadi kode ASCII dalam format heksadesimal, yang diformat dalam array berukuran 4 x 4 byte. Kemudian melakukan transformasi dasar seperti subbyte, migrasi, kolom campuran, addroundkey, dll. Namun, pada saat transformasi dilakukan, data saat itu sedang di proses setiap kali putaran merupakan bilangan binary yang diperoleh dari array heksadesimal. Pada Algoritma AES-128 byte memiliki nomor pengunci 128bit, Yakni, memiliki nilai lebih dari standar dan sudah aman untuk mencegah serangan serangan brutal.*

Received 01-01-2022
Revised 01-03-2022
Accepted 25-03-2022
Available online 01 -04-2022

***Keywords:*** *AES, AES algorithm, symmetric key algorithm, file encryption.*

***Abstract:*** *AES or the abbreviation of Cryptography Advanced Encryption Standard is used to encrypt files and documents. AES is a cryptographic algorithm which is an algorithm that encrypts the standard symmetric key used today. AES-128 has 1 block of 128-bit plaintext and the cryptographic algorithm process first converts the plaintext into a 4 x 4 hexadecimal array which can be called a state, where each state element is 1 bit in size. The process of encrypting into AES involves repeated state transitions in 10 steps. Each AES round requires only 1 result key from key generation using 2 transform keys, transform and replace. AES encryption uses 4 changes in the following order: sub-byte, shift, mixed field, and additional key. Instead, the decryption process uses the reverse of the basic transformation of the AES algorithm, except for an extra key. So the transformation order in the description is shiftrows, sub-bytes, mix column, and addroundkey. For text data, the encoding process begins by converting the text data into ASCII code in hexadecimal format, which is formatted in a 4 x 4 byte array. It then performs basic transformations like subbytes, migrations, mixed fields, addroundkeys, etc. However, at the time the transformation is performed, the data currently being processed each time round is a binary number obtained from the hexadecimal array. The AES-128 byte algorithm has a 128-bit key number, Namely, it has more value than the standard and is safe to preventbrutal force attacks.*

## PENDAHULUAN

Saat ini, dengan pesatnya perkembangan teknologi dan informasi, orang dapat berkomunikasi satu sama lain dan bertukar informasi, dan waktu serta jarak tidak menghalangi komunikasi. Demikian pula, semakin banyak data yang dikirim, serta keamanan yang harus dimiliki teknologi Lebih berbahaya lagi jika Anda tidak terlindungi dari macam-macam ancaman yang ada di Internet. karena itulah, sekarang ada berbagai ilmu yang mempelajari keamanan data adalah ilmu yang mempelajari efek positif dari sistem permintaan informasi keamanan yang berfungsi untuk melindungi data yang dikirimkan. tentang cara keamanan data normal diketahui dari nama kriptografi .

Kriptografi adalah studi tentang metode aritmatika seperti validitas informasi, perpaduan informasi, dan otentikasi data terhubung dengan keamanan informasi dan informasi. Kriptografi adalah Perangkat yang mengubah pesan jelas (plaintext) menjadi pesan terenkripsi (ciphertext). Transformasi ini dikenal sebagai enkripsi (enkripsi). Dekripsi, di sisi lain, adalah proses mengubah ciphertext menjadi plaintext. Satu atau lebih pengunci kriptografi digunakan selama operasi enkripsi dan dekripsi.

Institut Standar dan Teknologi Nasional (NIST) memberi pemerintah federal AS standar kriptografi baru pada tahun 2000. *NIST* mengadakan kompetisi untuk membuat standar metode kriptografi baru, spesifikasinya ini akan dikenal sebagai Advanced Encryption Standard (AES).

Syarat-syarat untuk algoritma baru:

1. Termasuk kelompok algoritma kriptografi *simetris berdasarkan block cypher.*
2. Semua desain algoritme harus tersedia (tidak disembunyikan).
3. Fleksibilitas panjang pengunci: *128 btye, 192 byte ,* dan *256 btye* .
4. Setiap block ukuran terenkripsi adalah 128-bit.
5. Algoritma dapat diterapkan dengan baik pada *perangkat lunak* dan *perangkat keras*.

Sehingga didapatkanlah pemenang dari lomba tersebut: *Rijndae (***Joan Daemen** dan **Vincent Rijmen** – **Belgium**, dengan 86 opini).

Algoritma Rijndael memiliki spesifikasi:

- Rijndael Dapat mendukung fleksibilitas dengan Panjang pengunci 128-byte hingga 256-byte dalam peningkatan 32-byte.
- Ukuran blok dan Panjang pengunci dapat dipilih oleh diri sendiri
- Setiap blok terenkripsi pada nomor bilangan bulat tentu saja sama dengan ***DES***.
- Karena AES memilih panjang pegunci, yang dapat berupa salah satu dari 128, 192, dan 256 bit, diketahui bahwa AES menggunakan panjang pengunci tersebut.

## METODE PENELITIAN

Untuk mencari referensi pengumpulan data dan desain aplikasi yang sedang dibangun seperti dokumen, kriptografi, algoritma AES, dan MD5, salah satu tekniknya adalah dengan melakukan studi pustaka.

Studi dilakukan dengan menggunakan skenario pengujian untuk memvalidasi kelayakan algoritma kriptografi yang relevan serta pola dan fitur dari algoritma kriptografi yang terkait.

## HASIL DAN PEMBAHASAN

Katakanlah seseorang mengirim pesan dengan 128 byte, 16 byte, atau 16 karakter teks biasa yang terlihat seperti ini:

Teks biasa: UMT FTI
Pengunci: Adnan

Plaintext ini kemudian dimasukkan dalam keadaan seperti ini.

Teks biasa :

| | | | |
|---|---|---|---|
| U | F | (batal) | (batal) |
| M | T | (batal) | (batal) |
| T | I | (batal) | (batal) |
| (spasi) | (batal) | (batal) | (batal) |

Pengunci:

| | | | |
|---|---|---|---|
| A | N | (batal) | (batal) |
| D | (batal) | (batal) | (batal) |
| N | (batal) | (batal) | (batal) |
| A | (batal) | (batal) | (batal) |

AES menggunakan sistem representasi heksadesimal karena *menggunakan representasi byte*. Untuk mengonversi karakter teks di atas menjadi heksadesimal dengan melihat tabel KODE ASCII, Anda bisa mendapatkan.

Teks biasa :

| | | | |
|---|---|---|---|
| 4B | 74 | 00 | 00 |
| 72 | 6F | 00 | 00 |
| 69 | 67 | 00 | 00 |
| 00 | 00 | 00 | 00 |

Pengunci:

| | | | |
|---|---|---|---|
| 41 | 74 | 00 | 00 |
| 69 | 00 | 00 | 00 |
| 64 | 00 | 00 | 00 |
| 67 | 00 | 00 | 00 |

**Proses Ekspansi Pengunci**

Proses perluasan pengunci seperti berikut:

| | | | |
|---|---|---|---|
| 41 | 74 | 00 | 00 |
| 69 | 61 | 00 | 00 |
| 64 | 00 | 00 | 00 |
| 67 | 00 | 00 | 00 |

Dapat juga ditulis :

W0= 41 69 64 67
W1= 74 61 00 00
W2= 00 00 00 00
W3= 00 00 00 00

Jadi, inilah cara menemukan W4:

*Subkata W 4 = W 0 rotword (W 3) (RC [1]*
*= 41 69 64 67 (rotword (00 00 00 00)) adalah subkata ⊕ Subkata (00 00 00 00) dari 01 00 00 00:*
41 69 64 67 *01 00 00 00*
*=23 08 0A 16*

Hasil perhitungan untuk penambahan 1 ronde terdapat pada tabel berikut ini:

| ***W(i)*** | ***W(i-1)*** | ***Setelah subkata ⊕ rcon ⊕ Mengedip)*** |
|---|---|---|
| W4 | 00 00 00 00 | *23 08 0A 16* |
| W5 | *23 08 0A 16* | 4A 68 0A 16 |
| W6 | 4A 68 0A 16 | 4A 68 0A 16 |
| W7 | 4A 66 80A 16 | 4A 68 0A 16 |

**Proses Enkripsi**
Plainteks dan kunci pertama-tama harus di XOR bersama-sama sebagai berikut:

**Ronde 1**
a. Hasil dari Proses Subbyte (dapat memakai tabel s-box)

| | | | |
|---|---|---|---|
| 67 | A4 | EF | 83 |
| 47 | AB | 33 | 6E |
| 63 | 85 | F9 | ED |
| F2 | 40 | B7 | 63 |

b. Perubahan *Shift Rows*

| | | | |
|---|---|---|---|
| 67 | A4 | EF | 83 |
| 47 | AB | 33 | 6E |
| 63 | 85 | F9 | ED |
| F2 | 40 | B7 | 63 |

| | | | |
|---|---|---|---|
| 67 | A4 | EF | 83 |
| AB | 33 | 6E | 47 |
| F9 | ED | 63 | 85 |
| 63 | F2 | 40 | B7 |

c. MixColumn

Ada lebih banyak proses yang terlibat dalam putaran ini daripada proses lainnya. Karena dilakukan berbeda untuk setiap kolom kali ini, penulis memisahkan metode mixcolumns menjadi 4 bagian untuk matriks atau keadaan:

1. Proses *mixcolumn ke kolom pertama* .

$$\begin{bmatrix} S'(0,1) \\ S'(1,1) \\ S'(2,1) \\ S'(3,1) \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} 67 & A4 & EF & 83 \\ AB & 33 & 6E & 47 \\ F9 & ED & 63 & 85 \\ 63 & F2 & 40 & B7 \end{bmatrix}$$

$$= \begin{bmatrix} B2 & 19 & 54 & E6 \\ 59 & 1C & B8 & 2E \\ 80 & 5B & 87 & 17 \\ 3D & D6 & A7 & 29 \end{bmatrix}$$

Ciphertext yang akan digunakan sebagai input pada putaran kedua dikumpulkan pada putaran pertama. Ciphertext putaran kedua juga dapat digunakan sebagai input pada putaran ketiga. Prosedur tersebut diulangi hingga putaran ke-10. Hasil enkripsi untuk putaran ke-10 adalah sebagai berikut:

Babak 10:
Sub-Byte :

| | | | |
|---|---|---|---|
| D9 | 36 | 01 | 59 |
| EE | D4 | FF | 36 |
| EF | AD | D1 | AE |
| 2B | B7 | BC | 56 |

Shift-Baris:

| | | | |
|---|---|---|---|
| D9 | 36 | 01 | 59 |
| D4 | FF | 36 | EE |
| D1 | AE | EF | AD |
| 56 | 2B | B7 | BC |

Kunci tambahan:

| | | | |
|---|---|---|---|
| 9A | 79 | 9E | 64 |
| 53 | 8C | 31 | C2 |
| F4 | 99 | B6 | 38 |
| 59 | 64 | 64 | 68 |

Pada ronde ke 10 perubahan hanya ada 3 perubahan yaitu *Sub-byte*, *Shift-Rows, Addround-key.* Sehingga akan mendapatkan chipertext yang benar:x

Teks chiper:

| | | | |
|---|---|---|---|
| 9A | 79 | 9E | 64 |
| 53 | 8C | 31 | C2 |
| F4 | 99 | B6 | 38 |
| 59 | 64 | 64 | 68 |

jika didalam bentuk ASCII maka di dapat cipherteks: 2OkSXJxh1fH+u0fR0dgXeQ==

Mengubah menjadi terbalik dari setiap perubahan fundamental yang digunakan dalam algoritma AES digunakan dalam fase dekripsi untuk mengubah ciphertext kembali menjadi plaintext. L: inv-subbytes, inv-shiftrows, dan inv-mixcolumns adalah perubahan terbalik untuk setiap transformasi AES mendasar. Ditemukan dari prosedur deskripsi, yang melibatkan 10 putaran:

Teks biasa:

| | | | |
|---|---|---|---|
| 4B | 74 | 61 | 41 |
| 72 | 6F | 66 | 45 |
| 69 | 67 | 69 | 53 |
| 70 | 72 | 20 | 00 |

Plainteks yang dikonversi kedalam bentuk ASCII menjadi: “UMT FTI”. Dengan demikian, algoritma kriptografi AES pada:
teks biasa = “UMT FTI”
kunci = “Adnan”
Cipherteks yang didapatkan itu adalah =“2OkSXJxh1fH+u0fR0dgXeQ==”

## KESIMPULAN

Proses mengenkripsi jika menggunakan algoritma kriptografi AES 128 dan 128-byte (satu blok) plaintext untuk data teks pertama-tama penundaan dari kode heksadesimal ke ASCII dan dibuat sebagai larik 4x4 byte atau biasa disebut sebagai state. Proses mengenkripsi di AES-128 yakni *masa transisi yang diulang sebanyak 10 putaran.* Informasi yang diolah pada masing-masing putaran berupa informasi biner. Masing-masing putaran AES diperlukan hanya satu hasil pembentukan pengunci dan menggunakan 4 perubahan dasar*: subbyte, shift, kolom campuran, dan kunci tambahan. Proses dekripsi* berubah dalam urutan itu:
*inv-shiftrows, inv-subbytes, addround-key,* dan *inv-mixcolumns.*

Berkas dokumen yang dikonfirmasi berisi lebih dari 16 karakter dikodekan dan didekodekan setiap 16 karakter atau 128-byte. Dengan cara ini, Proses AES untuk mengenkripsi dan deskripsi berjalan secara bersamaan. Padding diterapkan ke file teks dengan kurang dari 16 karakter. Padding adalah penggunaan karakter ASCII yang hilang yang dapat diproses dan tidak mempengaruhi hasil encoding atau decoding.

Membantu encoding dan decoding MATLAB bisa jadi terorganisir dari cepat, benar dan efektif. Apa hanya diperlukan memasukkan teks biasa dan pengunci kemudian proses mengenkripsi dan mendekripsikan bisa jadi menghasilkan *pergi* dengan cepat

**REFERENSI**

Aditia Rahmat Tulloh (,2016). Kriptografi Advanced Enciption Standard (AES) Untuk Penyandian File Dokumen , Bandung :Universitas Islam.

Angga Aditya Permana (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Enciption Standard (AES) : Universitas Muhamadyah Tangerang

Arjana, PH dkk. (2012). Implementasi Enkripsi Data dengan Algoritma Vigenere Chiper . Sentika , (ISSN: 2089-9815).

Destriana, R., Husain, S. M., & Handayani, N. (2021). DIAGRAM UML DALAM MEMBUAT APLIKASI ANDROID FIREBASE" STUDI KASUS APLIKASI BANK SAMPAH".

Destriana, R., Handayani, N., Husain, S. M., & Siswanto, A. T. P. (2021, March). A Research to Design, Develop and Implementation of Android Application System for Waste Bank Sharia Community at Kampung Hijau Kemuning. In IOP Conference Series: Materials Science and Engineering (Vol. 1115, No. 1, p. 012042). IOP Publishing.

Destriana, R., Kom, M., Husain, S. M., Kom, S., Handayani, N., Kom, M., ... & Kom, S. (2021). Diagram *UML Dalam Membuat Aplikasi Android Firebase" Studi Kasus Aplikasi Bank Sampah"*. Deepublish.

Destriana, R. (2022). Enterprise Resource Planning Bagi Pemula (Teori dan Konseptual).

Destriana, R., Permana, A. A., Legawa, S. D., & Irawan, H. (2019, April). Security system development for vehicle using the method of “mail notification” at villa Rizki Ilhami Tangerang residential. In *IOP Conference Series: Materials* Science *and Engineering* (Vol. 508, No. 1, p. 012124). IOP Publishing.

Destriana, R., Nurnaningsih, D., Alamsyah, D., & Sinlae, A. A. J. (2021). Implementasi Metode Linear Discriminant Analysis (LDA) Pada Klasifikasi Tingkat Kematangan Buah Nanas. *Building of Informatics, Technology and Science (BITS)*, *3*(1), 56-63.

Kustiawan, D., Cholifah, W. N., Destriana, R., & Heriyani, N. (2022). Rancang Bangun Sistem Informasi Akuntansi Pengelolaan Koperasi Menggunakan Metode Extreme Programming. *Jurnal Teknologi dan Informasi*, *12*(1), 78-92.

Muhammad Taufiqur Rahman (2017). Perbandingan Perfomansi Algoritme Kriptografi Advanced Enciption Standard (AES) Dan Browifish Pada Teks di Platform Android. Universitas Brawijaya ISSN : 2548-964

Nugroho, N., Handayani, N., Destriana, R., & Ernawati, T. (2021). IMPLEMENTATION OF CERTAINTY FACTOR IN AN EXPERT SYSTEM FOR DIAGNOSING ORAL CANCER. *Jurnal Riset Informatika*, *4*(1), 79-86.

Permana, A. A., Taufiq, R., & Destriana, R. (2021). IMPLEMENTASI APLIKASI PENGAMANAN PESAN GAMBAR MENGGUNAKAN ALGORITMA ONE TIME PAD.

R Destriana dkk, 2018, Security system development for vehicle using the method of "mail notification" at villa Rizki Ilhami Tangerang, IOP Conference Series: Materials Science and Engineering, Volume 508.

Sri Mulyani. (2016). Metode Analisis dan Perancangan Sistem. Bandung: AbdiSistematika

Sianturi, FA, (2013). Perancangan Aplikasi Pengamanan Data Dengan Kriptografi Advanced Encryption Standard (AES) . , (ISSN: 2301-9425)

Luminita Defta (2010). Yang berjudul. Implementasi Algoritma AES Pada Pragraming Languages University Of Pitesti, ISSN : 1596-2490

Marwah K.Hussein (,2017). Enkripsi Gambar Stereo Setelah Kompresi oleh Advanced Enciption Standard (AES). Irak: Universitas Basrah.